

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

**MARIBEL FRANCO MORALES**

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA DE TELECOMUNICACIONES  
TURBO (ANTIOQUIA).  
2021

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

**MARIBEL FRANCO MORALES**

Diplomado de opción de grado presentado para optar el  
título de INGENIERA DE TELECOMUNICACIONES

DIRECTOR:  
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA DE TELECOMUNICACIONES  
TURBO (ANTIOQUIA).  
2021

NOTA DE ACEPTACIÓN:

---

---

---

---

---

---

---

---

Presidente del Jurado

---

Jurado

---

Jurado

Turbo (Antioquia), 29 de noviembre de 2021

## CONTENIDO

CONTENIDO .....	4
LISTA DE FIGURAS .....	6
GLOSARIO .....	11
RESUMEN .....	12
ABSTRACT .....	13
INTRODUCCIÓN .....	14
ESCENARIO PROPUESTO .....	15
Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces .....	16
Paso 1: Cablear la red como se muestra en la topología .....	16
Paso 2: Configurar los parámetros básicos para cada dispositivo. ....	17
Configuración R1 .....	17
Configuración R2 .....	18
Configuración R3 .....	19
Configuración D1 .....	20
Configuración D2 .....	22
Configuración A1 .....	24
Parte 2: Configurar la capa 2 de la red y el soporte de Host .....	26
Tarea 2.1 .....	27
Tarea 2.2 .....	28
Tarea 2.3 .....	29
Tarea 2.4 .....	30
Tarea 2.5 .....	31
Tarea 2.6 .....	32
Tarea 2.7 .....	34
Tarea 2.8 .....	35
Parte 3: Configurar los protocolos de enrutamiento .....	37
Tarea 3.1 .....	39
Tarea 3.2 .....	41
Tarea 3.3 .....	43
Tarea 3.4 .....	44
Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy) .....	46

Tarea 4.1 .....	49
Tarea 4.2 .....	49
Tarea 4.3 .....	50
Parte 5: Seguridad .....	53
Tarea 5.1 .....	54
Tarea 5.2 .....	55
Tarea 5.3 .....	56
Tarea 5.4 .....	57
Tarea 5.5 .....	59
Parte 6: Configure las funciones de Administración de Red .....	61
Tarea 6.1 .....	62
Tarea 6.2 .....	63
Tarea 6.3 .....	63
Tarea 6.4 .....	64
Tarea 6.5 .....	65
CONCLUSIONES .....	69
BIBLIOGRAFIA .....	70

## LISTA DE FIGURAS

Figura 1. Ilustración escenario propuesto .....	15
Figura 2. Conexión entre dispositivos .....	16
Figura 3: Verificación de servicios DHCP IPv4 en PC2 .....	34
Figura 4: Verificación de servicios DHCP IPv4 en PC3 .....	34
Figura 5: Verificación de conectividad en PC1 .....	35
Figura 6: Verificación de conectividad en PC2 .....	35
Figura 7: Verificación de conectividad en PC3 .....	36
Figura 8: Verificación de conectividad en PC4 .....	36
Figura 9: Verificación de conectividad desde D1 a Loopback0.....	45
Figura 10: Verificación de conectividad desde D2 a Loopback0.....	45

## LISTA DE TABLAS

Tabla 1: Direccionamiento .....	15
Tabla 2: Tareas Parte 2 .....	26
Tabla 3: Tareas Parte 2 (continuación).....	27
Tabla 4: Tareas Parte 3 .....	38
Tabla 5: Tareas Parte 3 (continuación).....	39
Tabla 6: Tareas Parte 4 .....	46
Tabla 7: Tareas Parte 4 (continuación).....	47
Tabla 8: Tareas Parte 4 (continuación).....	48
Tabla 9: Tareas Parte 5 .....	53
Tabla 11: Tareas Parte 6 .....	61

## GLOSARIO

**LAN:** Local Area Network, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).

**WAN:** Wide Area Network (“Red de Área Amplia”). El concepto se utiliza para nombrar a la red de computadoras que se extiende en una gran franja de territorio, ya sea a través de una ciudad, un país o, incluso, a nivel mundial.

**NAT:** (Network Address Translation ó Traducción de Dirección de Red) es un mecanismo utilizado por routers y equipos para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles.

**VLAN:** (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física. Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física.

**DHCP:** (Dynamic Host Configuration Protocol). Protocolo de configuración dinámica de host. Protocolo que usan las computadoras para obtener información de configuración. El DHCP permite asignar una dirección IP a una computadora sin requerir que un administrador configure la información sobre la computadora en la base de datos de un servidor.

**DNS:** Domain Name System” (sistema de nombre de dominio). DNS es un servicio que habilita un enlace entre nombres de dominio y direcciones IP con la que están asociados.

**OSPF:** Open Shortest Path First (OSPF) es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF).

**IP:** La dirección IP es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, teléfono inteligente) que utilice el protocolo o (Internet Protocol).

**SERVIDOR:** Un servidor es un ordenador u otro tipo de equipo informático encargado de suministrar información a una serie de clientes, que pueden ser tanto personas como otros dispositivos conectados a él. La información que puede transmitir es múltiple y variada: desde archivos de texto, imagen o vídeo y hasta programas informáticos, bases de datos, etc.



## RESUMEN

El siguiente trabajo sobre redes en CCNP, se trata de la solución de un escenario con 6 partes a desarrollar, en la primera se construye la topología, se configura lo básico en cada dispositivo y el direccionamiento de las interfaces en la segunda parte, se configura la capa 2 de red y el soporte de host, para la tercera parte se configuran los protocolos de enrutamiento, seguidamente en la cuarta parte, se configura la redundancia del primer salto, posteriormente la seguridad en la quinta parte y finalmente en la parte 6 se configuran algunas características de administración de red.

Los protocolos de enrutamiento utilizados en este trabajo final de CISCO CCNP, son, por ejemplo, BGP, que no es más que un protocolo de enrutamiento entre sistemas autónomos, es muy utilizado por proveedores de servicios de internet.

En la parte 2 se emplea LACP para aumentar la capacidad de conmutación, ya que, como lo sabemos, gracias a la agregación de enlaces, podemos además dar redundancia, en el caso de que uno de los enlaces falle, pues tanto el software como la electrónica utilizada en los equipos de comunicación está orientada a cubrir esta necesidad de soporte a fallos.

Palabras clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

## ABSTRACT

The following work on networks in CCNP is about the solution of a scenario with 6 parts to be developed, in the first the topology is built, the basics are configured in each device and the addressing of the interfaces in the second part, it is configured the network layer 2 and the host support, for the third part the routing protocols are configured, then in the fourth part, the redundancy of the first hop is configured, then the security in the fifth part and finally in the part 6 configure some network management features.

The routing protocols used in this final CISCO CCNP work are, for example, BGP, which is nothing more than a routing protocol between autonomous systems, it is widely used by internet service providers.

In part 2 LACP is used to increase the switching capacity, since, as we know, thanks to the aggregation of links, we can also provide redundancy, in the event that one of the links fails, since both the software and the electronics used in communication equipment are aimed at meeting this need for fault support.

Keywords: CISCO, CCNP, Switching, Routing, Networks, Electronics.

## INTRODUCCIÓN

Este trabajo se refiere al desarrollo construcción de un escenario en el cual, primero construimos la topología de la red, luego, configuramos el enrutamiento, con esto se logra que los dispositivos en distintas redes se comuniquen, seguidamente, se configura la redundancia del último salto con HSRP, cuando todo lo anterior se encuentra configurado, le damos seguridad de acceso a los dispositivos y por último configuramos lo necesario para poder administrar los equipos desplegados.

Este escenario se implementó en GNS3, a continuación, siguiendo lo solicitado en la primera parte, en la cual se solicita mediante una tabla de direccionamiento, asignar direcciones tanto IP como IPV6, seguidamente, en la capa de red, es donde implementamos, como requerimiento de la parte 2, enlaces troncales, asignamos la VLAN nativa 999, se implementa el spanning tree, completamente importante en la capa 2 para evitar bucles, para este caso se empleó el rapid stp o RSTP, se fortalecieron los enlaces entre switches principales y de distribución con LACP. En la parte 3 se configuran los protocolos de enrutamiento OSPF y BGP en routers como en switches.

El desarrollo de la cuarta parte, implementa la redundancia del último salto, que con esto evitamos fallos en la salida de cada red, por algún fallo en una puerta de enlace, para esto, se requiere comprobar la disponibilidad de las salidas con IP SLA, luego con el protocolo HSRP, podemos tener esas redundancias necesarias para poder hacer la conmutación en caso de fallos. En la quinta parte realizamos las configuraciones de seguridad, que nos permitirán acceder a los dispositivos, ya sea autenticándonos localmente como a través de RADIUS. Por último, en la parte 6 configuramos las funciones de administración de red, muy necesarias, ellas son, NTP o network time protocol, éste, entrega la hora a los sistemas administrados, seguidamente configuramos el los mensajes syslog, que nos entregan información valiosa cada vez que ocurra una configuración nueva, un fallo o cualquier otro evento, quedará registrado. Ya para finalizar, configuramos el SNMP, en todos los dispositivos para poder administrarlos a través de Software diseñado para tal fin como Nagios, ManageEngine, por mencionar algunos.

*Figura 1. Ilustración escenario propuesto*

15

En esta prueba de habilidades, debe completar la configuración de la red para que haya una accesibilidad completa de un extremo a otro, para que los hosts tengan un soporte confiable de la puerta de enlace predeterminada (default gateway) y para que los protocolos configurados estén operativos dentro de la parte correspondiente a la "Red de la Compañía" en la topología. Tenga presente verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen como se requiere.

Procederemos entonces a realizar las configuraciones respectivas, teniendo en cuenta que hemos cambiado el nombre de las interfaces ya que lo desarrollamos en GNS3, pero la disposición de los routers y switches es exactamente la misma.

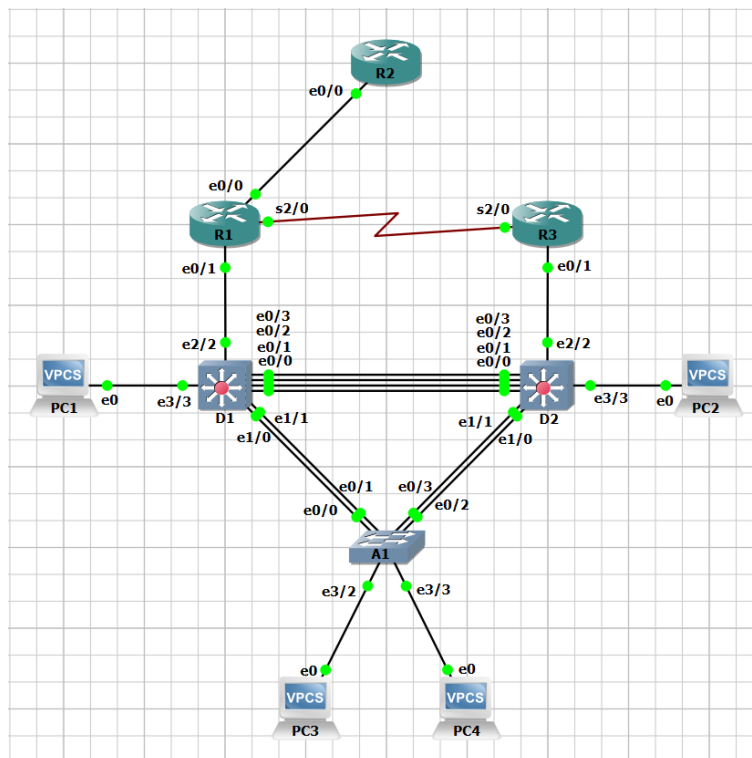
## Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces

### Paso 1: Cablear la red como se muestra en la topología.

Conecte los dispositivos como se muestra en el diagrama de topología y conecte los cables según sea necesario.

Se procede a realizar la implementación de la topología con cada uno de los switches y enrutadores propuestos, R1, R2, R3, D1, D2 y A1.

*Figura 2. Conexión entre dispositivos*



## Paso 2: Configurar los parámetros básicos para cada dispositivo.

- a. Mediante una conexión de consola ingrese en cada dispositivo, entre al modo de configuración global y aplique los parámetros básicos. Las configuraciones de inicio para cada dispositivo son suministradas a continuación:

Se realiza la configuración de los equipos de la topología, según el código suministrados en los enrutadores y switches R1, R2, R3, D1, D2 y A1.

### Configuración R1

Router> enable	ingreso al modo EXEC privilegiado
Router#configure terminal	entra al modo de configuración global
Router(config)#hostname R1	configuración del nombre del host
R1(config)#ipv6 unicast-routing	habilita enrutamiento con ipv6
R1(config)#no ip domain lookup	desactiva la traducción de nombres
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #	banner
R1(config)#line con 0	configuración de línea de consola
R1(config-line)# exec-timeout 0 0	desconexión por inactividad
R1(config-line)# logging synchronous	sincroniza logs
R1(config-line)# exit	salida de la configuración de la línea de consola
R1(config)#interface e0/0	entrada en la configuración de la interfaz
R1(config-if)# ip address 209.165.200.225 255.255.255.224	configuración ipv4
R1(config-if)# ipv6 address fe80::1:1 link-local	configura el enlace local ipv6
R1(config-if)# ipv6 address 2001:db8:200::1/64	configura ipv6
R1(config-if)# no shutdown	enciende la interfaz
R1(config-if)# exit	salida de la configuración de la interfaz
R1(config)#interface e0/1	entrada en la configuración de la interfaz
R1(config-if)# ip address 10.0.10.1 255.255.255.0	configuración de ipv4
R1(config-if)# ipv6 address fe80::1:2 link-local	configuración de enlace local ipv6
R1(config-if)# ipv6 address 2001:db8:100:1010::1/64	configuración de ipv6
R1(config-if)# no shutdown	enciende la interfaz
R1(config-if)# exit	salida de la configuración de la interfaz
R1(config)#interface s2/0	entrada en la configuración de la interfaz
R1(config-if)# ip address 10.0.13.1 255.255.255.0	configuración ipv4

R1(config-if)# ipv6 address fe80::1:3 link-local	configuración enlace local ipv6
R1(config-if)# ipv6 address 2001:db8:100:1013::1/64	configuración ipv6
R1(config-if)# no shutdown	enciende la interfaz
R1(config-if)# exit	salida de la configuración de la interfaz
R1(config)#end	sale al modo EXEC privilegiado
R1#copy running-config startup-config	salva la configuración

## Configuración R2

Router> enable	ingreso al modo EXEC privilegiado
Router#configure terminal	entra al modo de configuración global
Router(config)#hostname R2	configuración del nombre del host
R2(config)#ipv6 unicast-routing	habilita el ipv6
R2(config)#no ip domain lookup	desactiva la traducción de nombres
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 #	banner
R2(config)#line con 0	configura la línea de consola
R2(config-line)# exec-timeout 0 0	desconexión por inactividad
R2(config-line)# logging synchronous	sincroniza logs
R2(config-line)# exit	salida de la configuración de la línea de consola
R2(config)#interface e0/0	entrada en la configuración de la interfaz
R2(config-if)# ip address 209.165.200.226 255.255.255.224	configuración ipv4
R2(config-if)# ipv6 address fe80::2:1 link-local	configuración de enlace local ipv6
R2(config-if)# ipv6 address 2001:db8:200::2/64	configuración ipv6
R2(config-if)# no shutdown	encendido de la interfaz
R2(config-if)# exit	salida de la configuración de la interfaz
R2(config)#interface Loopback 0	configuración de interfaz virtual Loopback0
R2(config-if)# ip address 2.2.2.2 255.255.255.255	configuración ipv4
R2(config-if)# ipv6 address fe80::2:3 link-local	configuración de enlace local ipv6
R2(config-if)# ipv6 address 2001:db8:2222::1/128	configuración ipv6
R2(config-if)# no shutdown	encendido de la interfaz
R2(config-if)# exit	salida de la configuración de la interfaz
R2(config)#end	sale al modo EXEC privilegiado

R2#copy running-config startup-config

salva la configuración

### Configuración R3

Router> enable

ingreso al modo EXEC privilegiado

Router#configure terminal

entra al modo de configuración global

Router(config)#hostname R3

configuración del nombre del host

R3(config)#ipv6 unicast-routing

habilita enrutamiento con ipv6

R3(config)#no ip domain lookup

desactiva la traducción de nombres

R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #

banner

R3(config)#line con 0

configuración de línea de consola

R3(config-line)# exec-timeout 0 0

desconexión por inactividad

R3(config-line)# logging synchronous

sincroniza logs

R3(config-line)# exit

salida de la configuración de la línea de consola

R3(config)#interface e0/1

entrada en la configuración de la interfaz

R3(config-if)# ip address 10.0.11.1 255.255.255.0

configuración ipv4

R3(config-if)# ipv6 address fe80::3:2 link-local

configuración de enlace local ipv6

R3(config-if)# ipv6 address 2001:db8:100:1011::1/64

configuración ipv6

R3(config-if)# no shutdown

encendido de la interfaz

R3(config-if)# exit

salida de la configuración de la interfaz

R3(config)#interface s2/0

entrada en la configuración de la interfaz

R3(config-if)# ip address 10.0.13.3 255.255.255.0

configuración ipv4

R3(config-if)# ipv6 address fe80::3:3 link-local

configuración de enlace local ipv6

R3(config-if)# ipv6 address 2001:db8:100:1010::2/64

configuración ipv6

R3(config-if)# no shutdown

encendido de la interfaz

R3(config-if)# exit

salida de la configuración de la interfaz

R3(config)#end

sale al modo EXEC privilegiado

R3#copy running-config startup-config

guarda la configuración en la flash



## Configuración D1

Switch>enable	ingreso al modo EXEC privilegiado
Switch#configure terminal	entra al modo de configuración global
Switch(config)#hostname D1	configuración nombre del host
D1(config)#ip routing	habilita el enrutamiento en el switch
D1(config)#ipv6 unicast-routing	habilita el enrutamiento ipv6 en el switch
D1(config)#no ip domain lookup	desactiva la traducción de nombres
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1 #	banner
D1(config)#line con 0	configuración de línea de consola
D1(config-line)# exec-timeout 0 0	desconexión por inactividad
D1(config-line)# logging synchronous	sincroniza logs
D1(config-line)# exit	salida de la configuración de la línea de consola
D1(config)#vlan 100	configuración de vlan 100
D1(config-vlan)# name Management	nombramiento de la vlan
D1(config-vlan)# exit	salida de la configuración de la vlan
D1(config)#vlan 101	configuración de vlan 101
D1(config-vlan)# name UserGroupA	nombramiento de la vlan
D1(config-vlan)# exit	salida de la configuración de la vlan
D1(config)#vlan 102	configuración de vlan 102
D1(config-vlan)# name UserGroupB	nombramiento de la vlan
D1(config-vlan)# exit	salida de la configuración de la vlan
D1(config)#vlan 999	configuración vlan 999
D1(config-vlan)# name NATIVE	nombramiento de la vlan
D1(config-vlan)# exit	salida de la configuración de la vlan
D1(config)#interface e2/2	entrada en la configuración de la interfaz
D1(config-if)# no switchport	habilitación como puerto de router
D1(config-if)# ip address 10.0.10.2 255.255.255.0	asignación de dirección ip
D1(config-if)# ipv6 address fe80::d1:1 link-local	configuración de link local
D1(config-if)# ipv6 address 2001:db8:100:1010::2/64	configuración de ipv6
D1(config-if)# no shutdown	encendido de la interfaz
D1(config-if)# exit	salida de la interfaz

D1(config)#interface vlan 100      entrada en la configuración de interfaz de vlan 100  
D1(config-if)# ip address 10.0.100.1 255.255.255.0      asignación de IP en vlan 100  
D1(config-if)# ipv6 address fe80::d1:2 link-local      configuración de link local  
D1(config-if)# ipv6 address 2001:db8:100:100::1/64      configuración de ipv6  
D1(config-if)# no shutdown      encendido de la interfaz  
D1(config-if)# exit      salida de interfaz vlan  
D1(config)#interface vlan 101      entrada en la interfaz vlan 101  
D1(config-if)# ip address 10.0.101.1 255.255.255.0      asignación de IP en vlan 101  
D1(config-if)# ipv6 address fe80::d1:3 link-local      configuración de link local  
D1(config-if)# ipv6 address 2001:db8:100:101::1/64      configuración de ipv6  
D1(config-if)# no shutdown      encendido de la interfaz  
D1(config-if)# exit      salida de la interfaz  
D1(config)#interface vlan 102      entrada en la interfaz vlan 102  
D1(config-if)# ip address 10.0.102.1 255.255.255.0      asignación de IP en vlan 102  
D1(config-if)# ipv6 address fe80::d1:4 link-local      configuración de link local  
D1(config-if)# ipv6 address 2001:db8:100:102::1/64      configuración de ipv6  
D1(config-if)# no shutdown      encendido de la interfaz  
D1(config-if)# exit      salida de la interfaz  
D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109      exclusión IP's  
D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254      exclusión IP's  
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109      exclusión IP's  
D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254      exclusión IP's  
D1(config)#ip dhcp pool VLAN-101      configuración del pool dhcp en la vlan 101  
D1(dhcp-config)# network 10.0.101.0 255.255.255.0      configuración red del pool  
D1(dhcp-config)# default-router 10.0.101.254      configuración de gateway del pool  
D1(dhcp-config)# exit      salida de la configuración del pool  
D1(config)#ip dhcp pool VLAN-102      configuración del pool dhcp en la vlan 101  
D1(dhcp-config)# network 10.0.102.0 255.255.255.0      configuración red del pool  
D1(dhcp-config)# default-router 10.0.102.254      configuración de gateway del pool  
D1(dhcp-config)# exit      salida de la configuración del pool  
D1(config)#interface range e0/0-3, e1/0-3, e2/0-1, e2/3, e3/0-3 entrada en un rango de interfaces

D1(config-if-range)# shutdown	apagado de interfaces
D1(config-if-range)# exit	salida del rango de interfaces
D1(config)#end	sale al modo EXEC privilegiado
D1#copy running-config startup-config	salva la configuración

## Configuración D2

Switch>enable	ingreso al modo EXEC privilegiado
Switch#configure terminal	entra al modo de configuración global
Switch(config)#hostname D2	configuración del nombre del host
D2(config)#ip routing	habilita el enrutamiento en el switch
D2(config)#ipv6 unicast-routing	habilita el enrutamiento ipv6 en el switch
D2(config)#no ip domain lookup	desactiva la traducción de nombres
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 #	banner
D2(config)#line con 0	configuración de línea de consola
D2(config-line)# exec-timeout 0 0	desconexión por inactividad
D2(config-line)# logging synchronous	sincroniza logs
D2(config-line)# exit	salida de la configuración de la línea de consola
D2(config)#vlan 100	configuración de vlan 100
D2(config-vlan)# name Management	nombramiento de la vlan
D2(config-vlan)# exit	salida de la configuración de la vlan
D2(config)#vlan 101	configuración de vlan 101
D2(config-vlan)# name UserGroupA	nombramiento de la vlan
D2(config-vlan)# exit	salida de la configuración de la vlan
D2(config)#vlan 102	configuración de vlan 102
D2(config-vlan)# name UserGroupB	nombramiento de la vlan
D2(config-vlan)# exit	salida de la configuración de la vlan
D2(config)#vlan 999	configuración vlan 999
D2(config-vlan)# name NATIVE	nombramiento de la vlan
D2(config-vlan)# exit	salida de la configuración de la vlan
D2(config)#interface e2/2	entrada en la configuración de la interfaz
D2(config-if)# no switchport	habilitación como puerto de router

D2(config-if)# ip address 10.0.11.2 255.255.255.0	asignación de dirección ip
D2(config-if)# ipv6 address fe80::d1:1 link-local	configuración de link local
D2(config-if)# ipv6 address 2001:db8:100:1011::2/64	configuración de ipv6
D2(config-if)# no shutdown	encendido de la interfaz
D2(config-if)# exit	salida de la configuración de la vlan
D2(config)#interface vlan 100	entrada en la configuración de interfaz de vlan 100
D2(config-if)# ip address 10.0.100.2 255.255.255.0	asignación de IP en vlan 100
D2(config-if)# ipv6 address fe80::d2:2 link-local	configuración de link local
D2(config-if)# ipv6 address 2001:db8:100:100::2/64	configuración de ipv6
D2(config-if)# no shutdown	encendido de la interfaz
D2(config-if)# exit	salida de interfaz vlan
D2(config)#interface vlan 101	entrada en la interfaz vlan 101
D2(config-if)# ip address 10.0.101.2 255.255.255.0	asignación de IP en vlan 101
D2(config-if)# ipv6 address fe80::d2:3 link-local	configuración de link local
D2(config-if)# ipv6 address 2001:db8:100:101::2/64	configuración de ipv6
D2(config-if)# no shutdown	encendido de la interfaz
D2(config-if)# exit	salida de la interfaz
D2(config)#interface vlan 102	entrada en la interfaz vlan 102
D2(config-if)# ip address 10.0.102.2 255.255.255.0	asignación de IP en vlan 102
D2(config-if)# ipv6 address fe80::d2:4 link-local	configuración de link local
D2(config-if)# ipv6 address 2001:db8:100:102::2/64	configuración de ipv6
D2(config-if)# no shutdown	encendido de la interfaz
D2(config-if)# exit	salida de la interfaz
D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209	exclusión IP's
D2(config)#ip dhcp excluded-address 10.0.101.241 10.0.101.254	exclusión IP's
D2(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.209	exclusión IP's
D2(config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254	exclusión IP's
D2(config)#ip dhcp pool VLAN-101	configuración del pool dhcp en la vlan 101
D2(dhcp-config)# network 10.0.101.0 255.255.255.0	configuración red del pool
D2(dhcp-config)# default-router 10.0.101.254	configuración de gateway del pool
D2(dhcp-config)# exit	salida de la configuración del pool

D2(config)#ip dhcp pool VLAN-102	configuración del pool dhcp en la vlan 101
D2(dhcp-config)# network 10.0.102.0 255.255.255.0	configuración red del pool
D2(dhcp-config)# default-router 10.0.102.254	configuración de gateway del pool
D2(dhcp-config)# exit	salida de la configuración del pool
D2(config)#interface range e0/0-3, e1/0-3, e2/0-1, e2/3, e3/0-3	entrada en un rango de interfaces
D2(config-if-range)# shutdown	apagado de interfaces
D2(config-if-range)# exit	salida del rango de interfaces
D2(config)#end	sale al modo EXEC privilegiado
D2#copy running-config startup-config	salva la configuración

## Configuración A1

Switch>enable	ingreso al modo EXEC privilegiado
Switch#configure terminal	entra al modo de configuración global
Switch(config)#hostname A1	configuración nombre del host
A1(config)#no ip domain lookup	desactiva la traducción de nombres
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 #	banner
A1(config)#line con 0	configuración de línea de consola
A1(config-line)# exec-timeout 0 0	desconexión por inactividad
A1(config-line)# logging synchronous	sincroniza logs
A1(config-line)# exit	salida de la configuración de la línea de consola
A1(config)#vlan 100	configuración de vlan 100
A1(config-vlan)# name Management	nombramiento de la vlan
A1(config-vlan)# exit	salida de la configuración de la vlan
A1(config)#vlan 101	configuración de vlan 101
A1(config-vlan)# name UserGroupA	nombramiento de la vlan
A1(config-vlan)# exit	salida de la configuración de la vlan
A1(config)#vlan 102	configuración de vlan 102
A1(config-vlan)# name UserGroupB	nombramiento de la vlan
A1(config-vlan)# exit	salida de la configuración de la vlan
A1(config)#vlan 999	configuración vlan 999

A1(config-vlan)# name NATIVE	nombramiento de la vlan
A1(config-vlan)# exit	salida de la configuración de la vlan
A1(config)#interface vlan 100	entrada en la configuración de interfaz de vlan 100
A1(config-if)# ip address 10.0.100.3 255.255.255.0	asignación de IP en vlan 100
A1(config-if)# ipv6 address fe80::a1:1 link-local	configuración de link local
A1(config-if)# ipv6 address 2001:db8:100:100::3/64	configuración de ipv6
A1(config-if)# no shutdown	encendido de la interfaz
A1(config-if)# exit	salida de la interfaz
A1(config)#interface range e0/0-3, e1/0-3, e2/0-3, e3/0-1	entrada en un rango de interfaces
A1(config-if-range)# shutdown	apagado de interfaces
A1(config-if-range)# exit	salida del rango de interfaces
A1(config)#end	sale al modo EXEC privilegiado
A1#copy running-config startup-config	salva la configuración

- a. Copie el archivo running-config al archivo startup-config en todos los dispositivos.
- b. Configure el direccionamiento de los host PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.0.100.254, la cual será la dirección IP virtual HSRP utilizada en la Parte 4.

## Parte 2: Configurar la capa 2 de la red y el soporte de Host

En esta parte de la prueba de habilidades, debe completar la configuración de la capa 2 de la red y establecer el soporte básico de host. Al final de esta parte, todos los switches deben poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

Las tareas de configuración son las siguientes:

*Tabla 2: Tareas Parte 2*

Tarea#	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: <ul style="list-style-type: none"><li>• D1 and D2</li><li>• D1 and A1</li><li>• D2 and A1</li></ul>
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología.  D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: <ul style="list-style-type: none"><li>• D1 a D2 – Port channel 12</li><li>• D1 a A1 – Port channel 1</li><li>• D2 a A1 – Port channel 2</li></ul>
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología.  Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

*Tabla 3: Tareas Parte 2 (continuación)*

Tarea#	Tarea	Especificación
2.8	Verifique la conectividad de la LAN local	<p>PC1 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> <li>• D1: 10.0.100.1</li> <li>• D2: 10.0.100.2</li> <li>• PC4: 10.0.100.6</li> </ul> <p>PC2 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> <li>• D1: 10.0.102.1</li> <li>• D2: 10.0.102.2</li> </ul> <p>PC3 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> <li>• D1: 10.0.101.1</li> <li>• D2: 10.0.101.2</li> </ul> <p>PC4 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> <li>• D1: 10.0.100.1</li> <li>• D2: 10.0.100.2</li> <li>• PC1: 10.0.100.5</li> </ul>

### **Tarea 2.1**

Se realiza la configuración de las interfaces troncales en el switch D1, D2 y A1 se adjunta código:

#### **Configuración D1**

```

D1#configure terminal          entrada en el modo de configuración global
D1(config)#interface range e0/0-3      entrada en un rango de interfaces
D1(config-if-range)# switchport trunk encapsulation dot1q    tipo de encapsulación
D1(config-if-range)# switchport mode trunk                    modo de puerto
D1(config-if-range)# exit          salida del rango de interfaces
D1(config)#interface range e1/0-1  entrada en un rango de interfaces
D1(config-if-range)# switchport trunk encapsulation dot1q    tipo de encapsulación
D1(config-if-range)# switchport mode trunk                    modo de puerto
D1(config-if-range)# exit          salida del rango de interfaces
D1(config)#end              sale al modo EXEC privilegiado
D1#copy running-config startup-config      salva la configuración

```

#### **Configuración D2**

```

D2#configure terminal          entrada en el modo de configuración global
D2(config)#interface range e0/0-3      entrada en un rango de interfaces

```



D2(config-if-range)# switchport trunk encapsulation dot1q	tipo de encapsulación
D2(config-if-range)# switchport mode trunk	modo de puerto
D2(config-if-range)# exit	salida del rango de interfaces
D2(config)#interface range e1/0-1	entrada en un rango de interfaces
D2(config-if-range)# switchport trunk encapsulation dot1q	tipo de encapsulación
D2(config-if-range)# switchport mode trunk	modo de puerto
D2(config-if-range)# exit	salida del rango de interfaces
D2(config)#end	sale al modo EXEC privilegiado
D2#copy running-config startup-config	salva la configuración

### Configuración A1

A1#configure terminal	entrada en la configuración global
A1(config)#interface range e0/0-1	entrada en un rango de interfaces
A1(config-if-range)# switchport trunk encapsulation dot1q	tipo de encapsulación
A1(config-if-range)# switchport mode trunk	modo de puerto
A1(config-if-range)# exit	salida del rango de interfaces
A1(config)#interface range e0/2-3	entrada en un rango de interfaces
A1(config-if-range)# switchport trunk encapsulation dot1q	tipo de encapsulación
A1(config-if-range)# switchport mode trunk	modo de puerto
A1(config-if-range)# exit	salida del rango de interfaces
A1(config)#end	sale al modo EXEC privilegiado
A1#copy running-config startup-config	salva la configuración

### Tarea 2.2

Se procede con la configuración de la vlan nativa 999 en los puertos troncales en los switches D1, D2 y A1, se adjunta código:

### Configuración D1

D1#configure terminal	entrada en la configuración global
D1(config)#interface range e0/0-3	entrada en un rango de interfaces
D1(config-if-range)# switchport trunk native vlan 999	asignación de vlan nativa
D1(config-if-range)# exit	salida del rango de interfaces
D1(config)#interface range e1/0-1	entrada en un rango de interfaces

D1(config-if-range)# switchport trunk native vlan 999	asignación de vlan nativa
D1(config)#end	sale al modo EXEC privilegiado
D1#copy running-config startup-config	salva la configuración

### Configuración D2

D2#configure terminal	entrada en la configuración global
D2(config)#interface range e0/0-3	entrada en un rango de interfaces
D2(config-if-range)# switchport trunk native vlan 999	asignación de vlan nativa
D2(config-if-range)# exit	salida del rango de interfaces
D2(config)#interface range e1/0-1	entrada en un rango de interfaces
D2(config-if-range)# switchport trunk native vlan 999	asignación de vlan nativa
D2(config)#end	sale al modo EXEC privilegiado
D2#copy running-config startup-config	salva la configuración

### Configuración A1

A1#configure terminal	entrada en la configuración global
A1(config)#interface range e0/0-1	entrada en un rango de interfaces
A1(config-if-range)# switchport trunk native vlan 999	asignación de vlan nativa
A1(config-if-range)# exit	salida del rango de interfaces
A1(config)#interface range e0/2-3	entrada en un rango de interfaces
A1(config-if-range)# switchport trunk native vlan 999	asignación de vlan nativa
A1(config)#end	sale al modo EXEC privilegiado
A1#copy running-config startup-config	salva la configuración

### Tarea 2.3

Se procede a configurar en todos los switches el protocolo Rapid Spanning-Tree (RSTP), se adjunta código:

### Configuración D1

D1#configure terminal	entrada en la configuración global
D1(config)#spanning-tree mode rapid-pvst	modo de stp
D1(config)#end	sale al modo EXEC privilegiado
D1#copy running-config startup-config	salva la configuración

### **Configuración D2**

D2#configure terminal	entrada en la configuración global
D2(config)#spanning-tree mode rapid-pvst	modo de stp
D2(config)#end	sale al modo EXEC privilegiado
D2#copy running-config startup-config	salva la configuración

### **Configuración A1**

A1#configure terminal	entrada en la configuración global
A1(config)#spanning-tree mode rapid-pvst	modo de stp
A1(config)#end	sale al modo EXEC privilegiado
A1#copy running-config startup-config	salva la configuración

### **Tarea 2.4**

Se procede a configurar root bridge en switch D1 y D2, se adjunta código:

### **Configuración D1**

D1#configure terminal	entrada en la configuración global
D1(config)#spanning-tree vlan 100,102 root primary	raíz primaria de stp
D1(config)#spanning-tree vlan 101 root secondary	raíz secundaria de stp
D1(config)#end	sale al modo EXEC privilegiado
D1#copy running-config startup-config	salva la configuración

### **Configuración D2**

D2#configure terminal	entrada en la configuración global
D2(config)#spanning-tree vlan 101 root primary	raíz primaria de stp
D2(config)#spanning-tree vlan 100,102 root secondary	raíz secundaria de stp
D2(config)#end	sale al modo EXEC privilegiado
D2#copy running-config startup-config	salva la configuración

## Tarea 2.5

Se realiza la configuración de los port channel 1 y 2 en el switch D1, D2 y A1 y port channel 12 en switch D1 y D2 se adjunta código:

### Configuración D1

D1#configure terminal	entrada en la configuración global
D1(config)#interface range e0/0-3	entrada en un rango de interfaces
D1(config-if-range)# channel-group 12 mode active	creación del port channel
D1(config-if-range)# no shutdown	encendido el rango de interfaces
D1(config-if-range)# exit	salida del rango de interfaces
D1(config)#interface range e1/0-1	entrada en un rango de interfaces
D1(config-if-range)# channel-group 1 mode active	creación del port channel
D1(config-if-range)# exit	salida del rango de interfaces
D1(config)#end	sale al modo EXEC privilegiado
D1#copy running-config startup-config	salva la configuración

### Configuración D2

D2#configure terminal	entrada en la configuración global
D2(config)#interface range e0/0-3	entrada en un rango de interfaces
D2(config-if-range)# channel-group 12 mode active	creación del port channel
D2(config-if-range)# no shutdown	encendido el rango de interfaces
D2(config-if-range)# exit	salida del rango de interfaces
D2(config)#interface range e1/0-1	entrada en un rango de interfaces
D2(config-if-range)# channel-group 2 mode active	creación del port channel
D2(config-if-range)# exit	salida del rango de interfaces
D2(config)#end	sale al modo EXEC privilegiado
D2#copy running-config startup-config	salva la configuración

### Configuración A1

A1#configure terminal	entrada en la configuración global
A1(config)#interface range e0/0-1	entrada en un rango de interfaces
A1(config-if-range)# channel-group 1 mode active	creación del port channel
A1(config-if-range)# no shutdown	encendido el rango de interfaces

A1(config-if-range)# exit	salida del rango de interfaces
A1(config)#interface range e0/2-3	entrada en un rango de interfaces
A1(config-if-range)# channel-group 2 mode active	creación del port channel
A1(config-if-range)# exit	salida del rango de interfaces
A1(config)#end	sale al modo EXEC privilegiado
A1#copy running-config startup-config	salva la configuración

## Tarea 2.6

Se realiza la configuración de puertos de acceso en cada uno de los switches, se adjunta código:

### Configuración D1

D1#configure terminal	entrada en la configuración global
D1(config)#interface e3/3	entrada en la configuración de la interfaz
D1(config-if)# switchport mode access	modo del puerto
D1(config-if)# switchport access vlan 100	acceso del puerto a la vlan 100
D1(config-if)# spanning-tree portfast	stp para dispositivo terminal
D1(config-if)# no shutdown	encendido del puerto
D1(config-if)# exit	salida de la configuración del puerto
D1(config)#end	sale al modo EXEC privilegiado
D1#copy running-config startup-config	salva la configuración

### Configuración D2

D2#configure terminal	entrada en la configuración global
D2(config)#interface e3/3	entrada en la configuración de la interfaz
D2(config-if)# switchport mode access	modo del puerto
D2(config-if)# switchport access vlan 102	acceso del puerto a la vlan 102
D2(config-if)# spanning-tree portfast	stp para dispositivo terminal
D2(config-if)# no shutdown	encendido del puerto
D2(config-if)# exit	salida de la configuración del puerto
D2(config)#end	sale al modo EXEC privilegiado
D2#copy running-config startup-config	salva la configuración

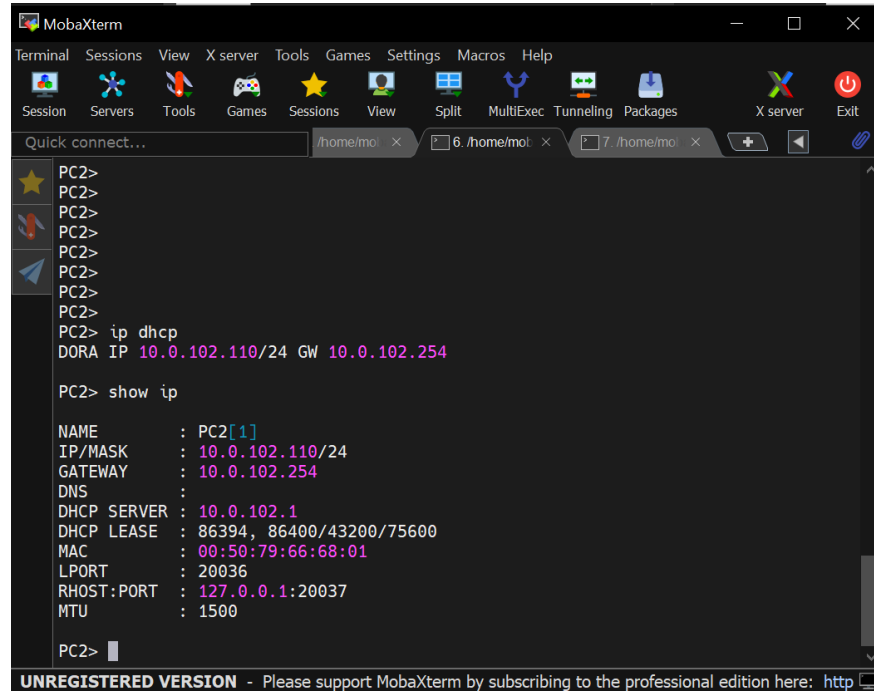
## Configuración A1

A1#configure terminal	entrada en la configuración global
A1(config)#interface e3/2	entrada en la configuración de la interfaz
A1(config-if)# switchport mode access	modo del puerto
A1(config-if)# switchport access vlan 101	acceso del puerto a la vlan 101
A1(config-if)# spanning-tree portfast	stp para dispositivo terminal
A1(config-if)# no shutdown	encendido del puerto
A1(config-if)# exit	salida de la configuración del puerto
A1(config)#interface e3/3	entrada en la configuración de la interfaz
A1(config-if)# switchport mode access	modo del puerto
A1(config-if)# switchport access vlan 102	acceso del puerto a la vlan 102
A1(config-if)# spanning-tree portfast	stp para dispositivo terminal
A1(config-if)# no shutdown	encendido del puerto
A1(config-if)# exit	salida de la configuración del puerto
A1(config)#end	sale al modo EXEC privilegiado
A1#copy running-config startup-config	salva la configuración

## Tarea 2.7

Se realiza la verificación del servicio DHCP en PC2 y PC3

*Figura 3: Verificación de servicios DHCP IPv4 en PC2*



The screenshot shows a MobaXterm terminal window with the following content:

```
MobaXterm
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages X server Exit

Quick connect... /home/mot x 6 /home/mot x 7 /home/mot x

PC2>
PC2>
PC2>
PC2>
PC2>
PC2>
PC2>
PC2> ip dhcp
DORA IP 10.0.102.110/24 GW 10.0.102.254

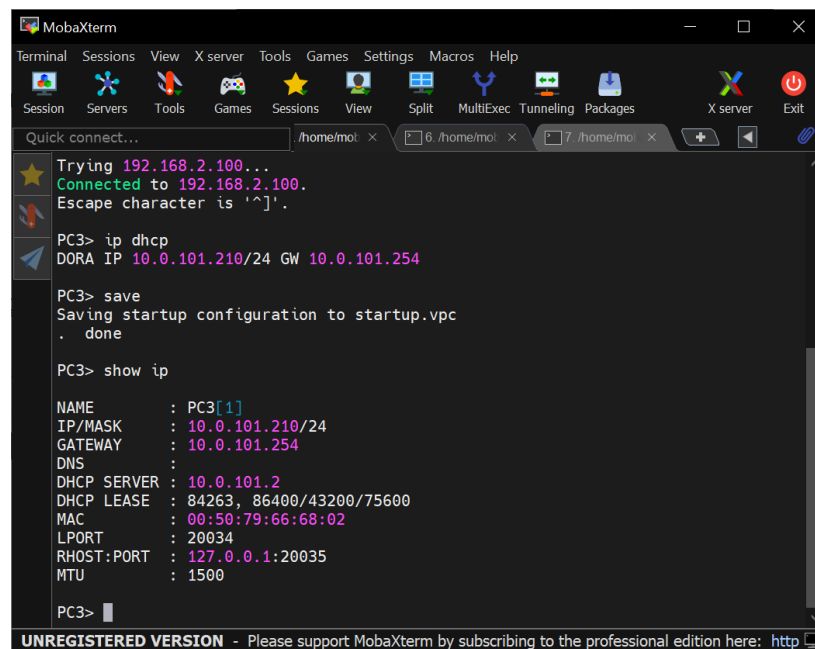
PC2> show ip

NAME      : PC2[1]
IP/MASK   : 10.0.102.110/24
GATEWAY   : 10.0.102.254
DNS       :
DHCP SERVER : 10.0.102.1
DHCP LEASE  : 86394, 86400/43200/75600
MAC        : 00:50:79:66:68:01
LPORT     : 20036
RHOST:PORT : 127.0.0.1:20037
MTU        : 1500

PC2>
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <http://>

*Figura 4: Verificación de servicios DHCP IPv4 en PC3*



The screenshot shows a MobaXterm terminal window with the following content:

```
MobaXterm
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages X server Exit

Quick connect... /home/mot x 6 /home/mot x 7 /home/mot x

Trying 192.168.2.100...
Connected to 192.168.2.100.
Escape character is '^]'.

PC3> ip dhcp
DORA IP 10.0.101.210/24 GW 10.0.101.254

PC3> save
Saving startup configuration to startup.vpc
. done

PC3> show ip

NAME      : PC3[1]
IP/MASK   : 10.0.101.210/24
GATEWAY   : 10.0.101.254
DNS       :
DHCP SERVER : 10.0.101.2
DHCP LEASE  : 84263, 86400/43200/75600
MAC        : 00:50:79:66:68:02
LPORT     : 20034
RHOST:PORT : 127.0.0.1:20035
MTU        : 1500

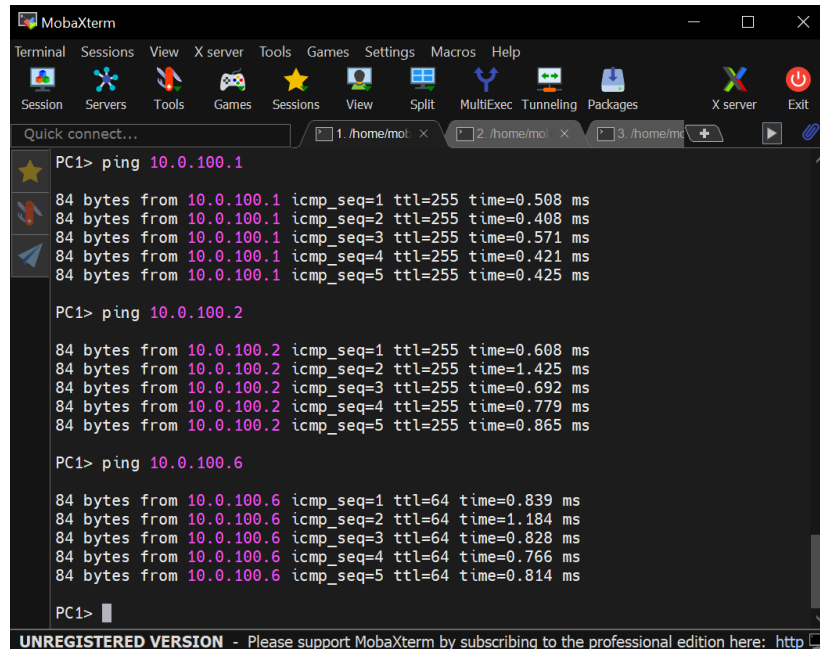
PC3>
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <http://>

## Tarea 2.8

Se realiza la verificación de conectividad en PC1, PC2, PC3 y PC4:

*Figura 5: Verificación de conectividad en PC1*



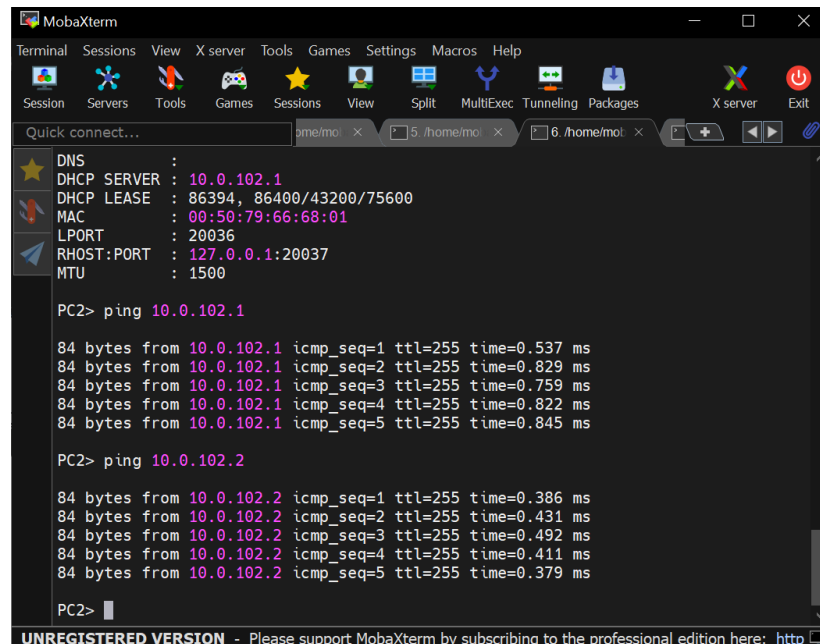
```
MobaXterm
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages X server Exit
Quick connect... [1] 1./home/mo... [2] 2./home/mo... [3] 3./home/mo...
PC1> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.508 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.408 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.571 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.421 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.425 ms

PC1> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.608 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=1.425 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=0.692 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=0.779 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=0.865 ms

PC1> ping 10.0.100.6
84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=0.839 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=1.184 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=0.828 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=0.766 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=0.814 ms

PC1>
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: http
```

*Figura 6: Verificación de conectividad en PC2*



```
MobaXterm
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages X server Exit
Quick connect... [5] 5./home/mo... [6] 6./home/mo...
DNS :
DHCP SERVER : 10.0.102.1
DHCP LEASE : 86394, 86400/43200/75600
MAC : 00:50:79:66:68:01
LPORT : 20036
RHOST:PORT : 127.0.0.1:20037
MTU : 1500

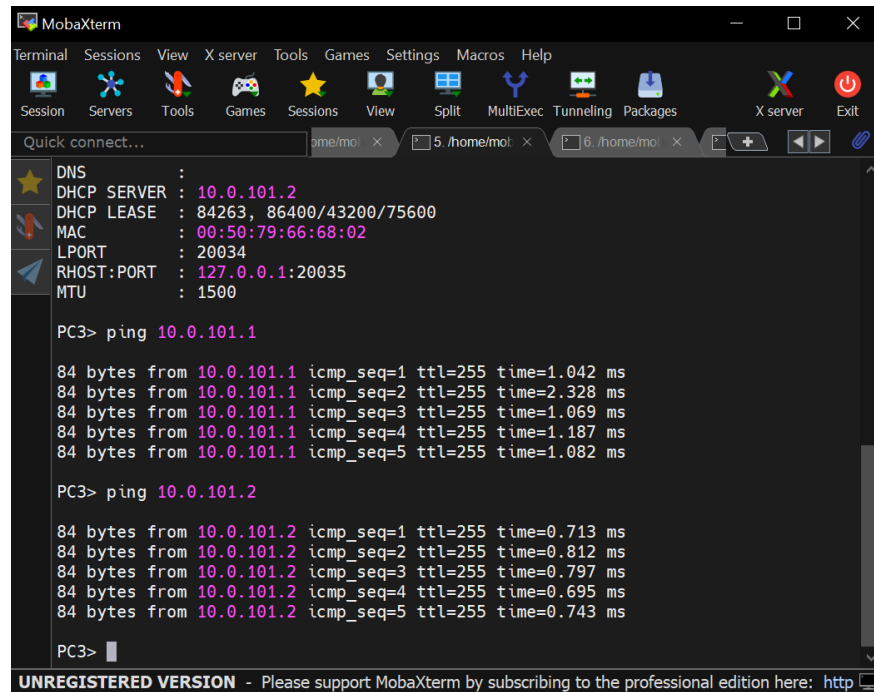
PC2> ping 10.0.102.1
84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=0.537 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=0.829 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=0.759 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=0.822 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=0.845 ms

PC2> ping 10.0.102.2
84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=0.386 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=0.431 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=0.492 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=0.411 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=0.379 ms

PC2>
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: http
```



Figura 7: Verificación de conectividad en PC3



The screenshot shows the MobaXterm application window. The terminal displays network configuration details for PC3, including DNS, DHCP server, lease, MAC address, LPORT, RHOST:PORT, and MTU. Below this, two ping commands are executed: 'ping 10.0.101.1' and 'ping 10.0.101.2'. Each ping command shows five successful responses with 84 bytes, TTL=255, and various response times in milliseconds. The terminal interface includes a menu bar (Terminal, Sessions, View, X server, Tools, Games, Settings, Macros, Help) and a toolbar with icons for Session, Servers, Tools, Games, Sessions, View, Split, MultiExec, Tunneling, Packages, X server, and Exit. The status bar at the bottom indicates 'UNREGISTERED VERSION' and provides a link to the professional edition.

```
MobaXterm
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages X server Exit
Quick connect... 5 /home/mo/ 6 /home/mo/
★ DNS :
DHCP SERVER : 10.0.101.2
DHCP LEASE : 84263, 86400/43200/75600
MAC : 00:50:79:66:68:02
LPORT : 20034
RHOST:PORT : 127.0.0.1:20035
MTU : 1500

PC3> ping 10.0.101.1

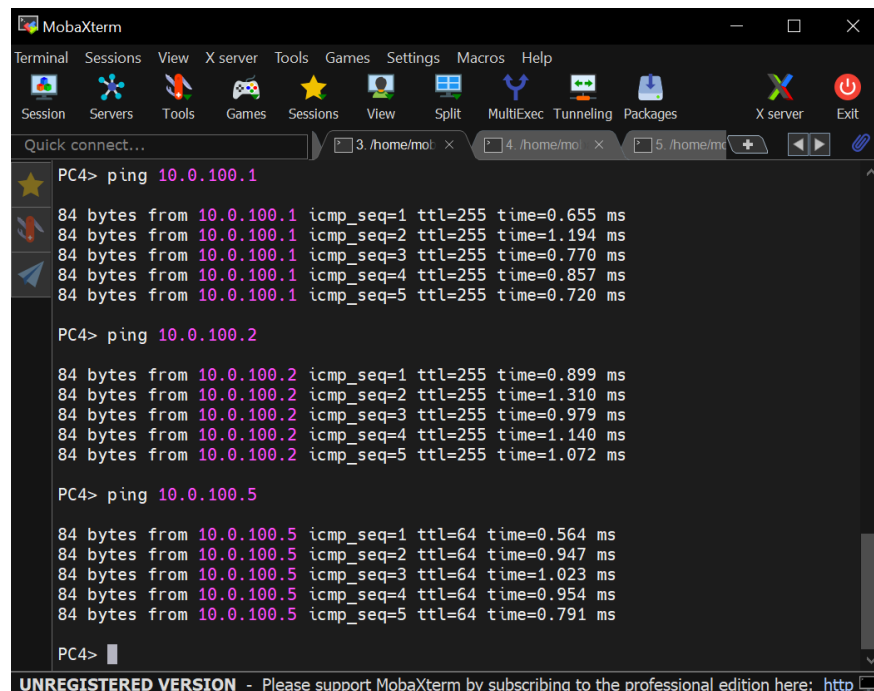
84 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=1.042 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=2.328 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=1.069 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=1.187 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=1.082 ms

PC3> ping 10.0.101.2

84 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=0.713 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=0.812 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=0.797 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=0.695 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=0.743 ms

PC3>
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: http
```

Figura 8: Verificación de conectividad en PC4



The screenshot shows the MobaXterm application window. The terminal displays network configuration details for PC4, including DNS, DHCP server, lease, MAC address, LPORT, RHOST:PORT, and MTU. Below this, three ping commands are executed: 'ping 10.0.100.1', 'ping 10.0.100.2', and 'ping 10.0.100.5'. Each ping command shows five successful responses with 84 bytes, TTL=255 (except for TTL=64 in the third command), and various response times in milliseconds. The terminal interface includes a menu bar (Terminal, Sessions, View, X server, Tools, Games, Settings, Macros, Help) and a toolbar with icons for Session, Servers, Tools, Games, Sessions, View, Split, MultiExec, Tunneling, Packages, X server, and Exit. The status bar at the bottom indicates 'UNREGISTERED VERSION' and provides a link to the professional edition.

```
MobaXterm
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages X server Exit
Quick connect... 3 /home/mo/ 4 /home/mo/ 5 /home/mo/
★ DNS :
DHCP SERVER : 10.0.100.1
DHCP LEASE : 84263, 86400/43200/75600
MAC : 00:50:79:66:68:02
LPORT : 20034
RHOST:PORT : 127.0.0.1:20035
MTU : 1500

PC4> ping 10.0.100.1

84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.655 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=1.194 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.770 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.857 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.720 ms

PC4> ping 10.0.100.2

84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.899 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=1.310 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=0.979 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=1.140 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=1.072 ms

PC4> ping 10.0.100.5

84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=0.564 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=0.947 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=1.023 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=0.954 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=0.791 ms

PC4>
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: http
```

### **Parte 3: Configurar los protocolos de enrutamiento**

En esta parte, debe configurar los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debería estar completamente convergente. Los pings de IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 deberían ser exitosos.

**Nota:** Los pings desde los hosts no tendrán éxito porque sus puertas de enlace predeterminadas apuntan a la dirección HSRP que se habilitará en la Parte 4.

Las tareas de configuración son las siguientes:

**Tabla 4: Tareas Parte 3**

Tarea#	Tarea	Especificación
3.1	En la "Red de la Compañía" (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en area 0.	<p>Use OSPF Process ID <b>4</b> y asigne los siguientes router-IDs:</p> <ul style="list-style-type: none"> <li>• R1: 0.0.4.1</li> <li>• R3: 0.0.4.3</li> <li>• D1: 0.0.4.131</li> <li>• D2: 0.0.4.132</li> </ul> <p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.</p> <ul style="list-style-type: none"> <li>• En R1, no publique la red R1 – R2.</li> <li>• En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.</li> </ul> <p>Deshabilite las publicaciones OSPFv2 en:</p> <ul style="list-style-type: none"> <li>• D1: todas las interfaces excepto G1/0/11</li> <li>• D2: todas las interfaces excepto G1/0/11</li> </ul>
3.2	En la "Red de la Compañía" (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	<p>Use OSPF Process ID <b>6</b> y asigne los siguientes router-IDs:</p> <ul style="list-style-type: none"> <li>• R1: 0.0.6.1</li> <li>• R3: 0.0.6.3</li> <li>• D1: 0.0.6.131</li> <li>• D2: 0.0.6.132</li> </ul> <p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.</p> <ul style="list-style-type: none"> <li>• En R1, no publique la red R1 – R2.</li> <li>• On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.</li> </ul> <p>Deshabilite las publicaciones OSPFv3 en:</p> <ul style="list-style-type: none"> <li>• D1: todas las interfaces excepto G1/0/11</li> <li>• D2: todas las interfaces excepto G1/0/11</li> </ul>
3.3	En R2 en la "Red ISP", configure MP-BGP.	<p>Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:</p> <ul style="list-style-type: none"> <li>• Una ruta estática predeterminada IPv4.</li> <li>• Una ruta estática predeterminada IPv6.</li> </ul> <p>Configure R2 en BGP ASN <b>500</b> y use el router-id 2.2.2.2.</p> <p>Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.</p> <p>En IPv4 address family, anuncie:</p> <ul style="list-style-type: none"> <li>• La red Loopback 0 IPv4 (/32).</li> <li>• La ruta por defecto (0.0.0.0/0).</li> </ul> <p>En IPv6 address family, anuncie:</p> <ul style="list-style-type: none"> <li>• La red Loopback 0 IPv4 (/128).</li> <li>• La ruta por defecto (::/0).</li> </ul>

*Tabla 5: Tareas Parte 3 (continuación)*

Tarea#	Tarea	Especificación
3.4	En R1 en la "Red ISP", configure MP-BGP.	<p>Configure dos rutas resumen estáticas a la interfaz Null 0:</p> <ul style="list-style-type: none"> <li>• Una ruta resumen IPv4 para 10.0.0.0/8.</li> <li>• Una ruta resumen IPv6 para 2001:db8:100::/48.</li> </ul> <p>Configure R1 en BGP ASN <b>300</b> y use el router-id 1.1.1.1.</p> <p>Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.</p> <p>En IPv4 address family:</p> <ul style="list-style-type: none"> <li>• Deshabilite la relación de vecino IPv6.</li> <li>• Habilite la relación de vecino IPv4.</li> <li>• Anuncie la red 10.0.0.0/8.</li> </ul> <p>En IPv6 address family:</p> <ul style="list-style-type: none"> <li>• Deshabilite la relación de vecino IPv4.</li> <li>• Habilite la relación de vecino IPv6.</li> <li>• Anuncie la red 2001:db8:100::/48.</li> </ul>

Se procede a configurar el enrutamiento tanto OSPF como BGP en los diferentes dispositivos, esta vez, solo en R1, R2, R3, D1 y D2, se adjunta código y pantallazos.

### Tarea 3.1

Se procede a configurar en la "Red de la Compañía" (es decir, R1, R3, D1, y D2), configure single- area OSPFv2 en area 0, se adjunta código:

#### Configuración R1

R1#configure terminal	entrada en la configuración global
R1(config)#router ospf 4	entrada en la configuración de ospf proceso 4
R1(config-router)# router-id 0.0.4.1	configuración ID de router
R1(config-router)# network 10.0.10.0 0.0.0.255 area 0	anuncio de red
R1(config-router)# network 10.0.13.0 0.0.0.255 area 0	anuncio de red
R1(config-router)# default-information originate	ruta por defecto
R1(config-router)# exit	salida de la configuración ospf
R1(config)#end	sale al modo EXEC privilegiado
R1#copy running-config startup-config	salva la configuración

### Configuración R3

R3#configure terminal	entrada en la configuración global
R3(config)#router ospf 4	entrada en la configuración de ospf proceso 4
R3(config-router)# router-id 0.0.4.3	configuración ID de router
R3(config-router)# network 10.0.11.0 0.0.0.255 area 0	anuncio de red
R3(config-router)# network 10.0.13.0 0.0.0.255 area 0	anuncio de red
R3(config-router)# exit	salida de la configuración ospf
R3(config)#end	sale al modo EXEC privilegiado
R3#copy running-config startup-config	salva la configuración

### Configuración D1

D1#configure terminal	entrada en la configuración global
D1(config)#router ospf 4	entrada en la configuración de ospf proceso 4
D1(config-router)# router-id 0.0.4.132	configuración ID de router
D1(config-router)# network 10.0.100.0 0.0.0.255 area 0	anuncio de red
D1(config-router)# network 10.0.101.0 0.0.0.255 area 0	anuncio de red
D1(config-router)# network 10.0.102.0 0.0.0.255 area 0	anuncio de red
D1(config-router)# network 10.0.10.0 0.0.0.255 area 0	anuncio de red
D1(config-router)# passive-interface default	interfaz pasiva predeterminada
D1(config-router)# no passive-interface e2/2	interfaz no pasiva
D1(config-router)# exit	salida de la configuración ospf
D1(config)#end	sale al modo EXEC privilegiado
D1#copy running-config startup-config	salva la configuración

### Configuración D2

D2#configure terminal	entrada en la configuración global
D2(config)#router ospf 4	entrada en la configuración de ospf proceso 4
D2(config-router)# router-id 0.0.4.131	configuración ID de router
D2(config-router)# network 10.0.100.0 0.0.0.255 area 0	anuncio de red
D2(config-router)# network 10.0.101.0 0.0.0.255 area 0	anuncio de red
D2(config-router)# network 10.0.102.0 0.0.0.255 area 0	anuncio de red

D2(config-router)# network 10.0.11.0 0.0.0.255 area 0	anuncio de red
D2(config-router)# passive-interface default	interfaz pasiva predeterminada
D2(config-router)# no passive-interface e2/2	interfaz no pasiva
D2(config-router)# exit	salida de la configuración ospf
D2(config)#end	sale al modo EXEC privilegiado
D2#copy running-config startup-config	salva la configuración

### Tarea 3.2

Se procede a configurar en la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single- area OSPFv3 en area 0, se adjunta código:

#### Configuración R1

R1#configure terminal	entrada en la configuración global
R1(config)#ipv6 router ospf 6	entrada en la configuración de ospf proceso 6
R1(config-rtr)# router-id 0.0.6.1	configuración ID de router
R1(config-rtr)# default-information originate	ruta por defecto
R1(config-rtr)# exit	salida de la configuración ospf
R1(config)#interface e0/1	entrada en interfaz
R1(config-if)# ipv6 ospf 6 area 0	configuración de ospf ipv6 proceso 6 area 0
R1(config-if)# exit	salida de la interfaz
R1(config)#interface s2/0	entrada en la interfaz
R1(config-if)# ipv6 ospf 6 area 0	configuración de ospf ipv6 proceso 6 area 0
R1(config-if)# exit	salida de la interfaz
R1(config)#end	sale al modo EXEC privilegiado
R1#copy running-config startup-config	salva la configuración

#### Configuración R3

R3#configure terminal	entrada en la configuración global
R3(config)#ipv6 router ospf 6	entrada en la configuración de ospf proceso 6
R3(config-rtr)# router-id 0.0.6.3	configuración ID de router
R3(config-rtr)# default-information originate	ruta por defecto
R3(config-rtr)# exit	salida de la configuración ospf
R3(config)#interface e0/1	entrada en interfaz

R3(config-if)# ipv6 ospf 6 area 0	configuración de ospf ipv6 proceso 6 area 0
R3(config-if)# exit	salida de la interfaz
R3(config)#interface s2/0	entrada en la interfaz
R3(config-if)# ipv6 ospf 6 area 0	configuración de ospf ipv6 proceso 6 area 0
R3(config-if)# exit	salida de la interfaz
R3(config)#end	sale al modo EXEC privilegiado
R3#copy running-config startup-config	salva la configuración

### Configuración D1

D1#configure terminal	entrada en la configuración global
D1(config)#ipv6 router ospf 6	entrada en la configuración de ospf proceso 6
D1(config-rtr)# router-id 0.0.6.131	configuración ID de router
D1(config-rtr)# passive-interface default	interfaz pasiva predeterminada
D1(config-rtr)# no passive-interface e2/2	interfaz no pasiva
D1(config-rtr)# exit	salida de la configuración ospf
D1(config)#interface e2/2	entrada en la interfaz
D1(config-if)# ipv6 ospf 6 area 0	configuración de ospf ipv6 proceso 6 area 0
D1(config-if)# exit	salida de la interfaz
D1(config)#interface vlan 100	entrada en la interfaz
D1(config-if)# ipv6 ospf 6 area 0	configuración de ospf ipv6 proceso 6 area 0
D1(config-if)# exit	salida de la interfaz
D1(config)#interface vlan 101	entrada en la interfaz
D1(config-if)# ipv6 ospf 6 area 0	configuración de ospf ipv6 proceso 6 area 0
D1(config-if)# exit	salida de la interfaz
D1(config)#interface vlan 102	entrada en la interfaz
D1(config-if)# ipv6 ospf 6 area 0	configuración de ospf ipv6 proceso 6 area 0
D1(config-if)# exit	salida de la interfaz
D1(config)#end	sale al modo EXEC privilegiado
D1#copy running-config startup-config	salva la configuración

## Configuración D2

D2#configure terminal	entrada en la configuración global
D2(config)#ipv6 router ospf 6	entrada en la configuración de ospf proceso 6
D2(config-rtr)# router-id 0.0.6.132	configuración ID de router
D2(config-rtr)# passive-interface default	interfaz pasiva predeterminada
D2(config-rtr)# no passive-interface e2/2	interfaz no pasiva
D2(config-rtr)# exit	salida de la configuración ospf
D2(config)#interface e2/2	entrada en la interfaz
D2(config-if)# ipv6 ospf 6 area 0	configuración de ospf ipv6 proceso 6 area 0
D2(config-if)# exit	salida de la interfaz
D2(config)#interface vlan 100	entrada en la interfaz
D2(config-if)# ipv6 ospf 6 area 0	configuración de ospf ipv6 proceso 6 area 0
D2(config-if)# exit	salida de la interfaz
D2(config)#interface vlan 101	entrada en la interfaz
D2(config-if)# ipv6 ospf 6 area 0	configuración de ospf ipv6 proceso 6 area 0
D2(config-if)# exit	salida de la interfaz
D2(config)#interface vlan 102	entrada en la interfaz
D2(config-if)# ipv6 ospf 6 area 0	configuración de ospf ipv6 proceso 6 area 0
D2(config-if)# exit	salida de la interfaz
D2(config)#end	sale al modo EXEC privilegiado
D2#copy running-config startup-config	salva la configuración

## Tarea 3.3

Se procede a configurar en R2 en la "Red ISP", configure MP - BGP, se adjunta código:

## Configuración R2

R2#configure terminal	entrada en la configuración global
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0	configuración ipv4 loopback 0
R2(config)#ipv6 route ::/0 loopback 0	configuración ipv6 loopback 0
R2(config)#router bgp 500	configuración bgp
R2(config-router)# bgp router-id 2.2.2.2	ID de router bgp
R2(config-router)# neighbor 209.165.200.225 remote-as 300	vecino ipv4



R2(config-router)# neighbor 2001:db8:200::1 remote-as 300	vecino ipv6
R2(config-router)# address-family ipv4	configuración familia
R2(config-router-af)# neighbor 209.165.200.225 activate	habilitación vecino
R2(config-router-af)# no neighbor 2001:db8:200::1 activate	deshabilitación vecino
R2(config-router-af)# network 2.2.2.2 mask 255.255.255.255	anuncio de red
R2(config-router-af)# network 0.0.0.0	anuncio de red
R2(config-router-af)# exit-address-family	salida configuración familia
R2(config-router)# address-family ipv6	configuración familia
R2(config-router-af)# no neighbor 209.165.200.225 activate	deshabilitación vecino
R2(config-router-af)# neighbor 2001:db8:200::1 activate	habilitación vecino
R2(config-router-af)# network 2001:db8:2222::/128	anuncio de red
R2(config-router-af)# network ::/0	anuncio de red
R2(config-router-af)# exit-address-family	salida configuración familia
R2(config-router)#end	sale al modo EXEC privilegiado
R2#copy running-config startup-config	salva la configuración

### Tarea 3.4

Se procede a configurar en R1 en la “Red ISP”, configure MP - BGP, se adjunta código:

#### Configuración R1

R1#configure terminal	entrada en la configuración global
R1(config)#ip route 10.0.0.0 255.0.0.0 null0	configuración de ruta
R1(config)#ipv6 route 2001:db8:100::/48 null0	configuración de ruta
R1(config)#router bgp 300	configuración de bgp
R1(config-router)# bgp router-id 1.1.1.1	configuración de ID de bgp
R1(config-router)# neighbor 209.165.200.226 remote-as 500	vecino ipv4
R1(config-router)# neighbor 2001:db8:200::2 remote-as 500	vecino ipv6
R1(config-router)# address-family ipv4 unicast	configuración familia
R1(config-router-af)# neighbor 209.165.200.226 activate	habilitación vecino
R1(config-router-af)# no neighbor 2001:db8:200::2 activate	deshabilitación vecino
R1(config-router-af)# network 10.0.0.0 mask 255.0.0.0	anuncio de red
R1(config-router-af)# exit-address-family	salida configuración familia

R1(config-router)# address-family ipv6 unicast	configuración familia
R1(config-router-af)# no neighbor 209.165.200.226 activate	deshabilitación vecino
R1(config-router-af)# neighbor 2001:db8:200::2 activate	habilitación vecino
R1(config-router-af)# network 2001:db8:100::/48	anuncio de red
R1(config-router-af)# exit-address-family	salida configuración familia
R1(config-router)# end	sale al modo EXEC privilegiado
R1#copy running-config startup-config	salva la configuración

*Figura 9: Verificación de conectividad desde D1 a Loopback0*

```

D1#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
D1#ping 2001:db8:2222::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:2222::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/18 ms
D1#

```

*Figura 10: Verificación de conectividad desde D2 a Loopback0*

```

D2#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/10 ms
D2#ping 2001:db8:2222::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:2222::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/13/28 ms
D2#

```

#### Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)

En esta parte, debe configurar HSRP versión 2 para proveer redundancia de primer salto para los hosts en la “Red de la Compañía”.

Las tareas de configuración son las siguientes:

*Tabla 6: Tareas Parte 4*

Tarea#	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.	<p>Cree dos IP SLAs.</p> <ul style="list-style-type: none"><li>• Use la SLA número <b>4</b> para IPv4.</li><li>• Use la SLA número <b>6</b> para IPv6.</li></ul> <p>Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos.</p> <p>Programe la SLA para una implementación inmediata sin tiempo de finalización.</p> <p>Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.</p> <ul style="list-style-type: none"><li>• Use el número de rastreo <b>4</b> para la IP SLA 4.</li><li>• Use el número de rastreo <b>6</b> para la IP SLA 6.</li></ul> <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>
4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.	<p>Cree IP SLAs.</p> <ul style="list-style-type: none"><li>• Use la SLA número <b>4</b> para IPv4.</li><li>• Use la SLA número <b>6</b> para IPv6.</li></ul> <p>Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos.</p> <p>Programe la SLA para una implementación inmediata sin tiempo de finalización.</p> <p>Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.</p> <ul style="list-style-type: none"><li>• Use el número de rastreo <b>4</b> para la IP SLA 4.</li><li>• Use el número de rastreo <b>6</b> para la SLA 6.</li></ul> <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>

*Tabla 7: Tareas Parte 4 (continuación)*

Tarea#	Tarea	Especificación
4.3	En D1 configure HSRPv2.	<p>D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150..</p> <p>Configure HSRP version 2.</p> <p>Configure IPv4 HSRP grupo <b>104</b> para la VLAN 100:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual <b>10.0.100.254</b>.</li> <li>• Establezca la prioridad del grupo en <b>150</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 y decremente en 60.</li> </ul> <p>Configure IPv4 HSRP grupo <b>114</b> para la VLAN 101:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual <b>10.0.101.254</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 para disminuir en 60.</li> </ul> <p>Configure IPv4 HSRP grupo <b>124</b> para la VLAN 102:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual <b>10.0.102.254</b>.</li> <li>• Establezca la prioridad del grupo en <b>150</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 para disminuir en 60.</li> </ul> <p>Configure IPv6 HSRP grupo <b>106</b> para la VLAN 100:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6 autoconfig</b>.</li> <li>• Establezca la prioridad del grupo en <b>150</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 6 y decremente en 60.</li> </ul> <p>Configure IPv6 HSRP grupo <b>116</b> para la VLAN 101:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6 autoconfig</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Registre el objeto 6 y decremente en 60.</li> </ul> <p>Configure IPv6 HSRP grupo <b>126</b> para la VLAN 102:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6 autoconfig</b>.</li> <li>• Establezca la prioridad del grupo en <b>150</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 6 y decremente en 60.</li> </ul>

**Tabla 8: Tareas Parte 4 (continuación)**

Tarea#	Tarea	Especificación
	En D2, configure HSRPv2.	<p>D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150.</p> <p>Configure HSRP version 2.</p> <p>Configure IPv4 HSRP grupo <b>104</b> para la VLAN 100:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual <b>10.0.100.254</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 y decremente en 60.</li> </ul> <p>Configure IPv4 HSRP grupo <b>114</b> para la VLAN 101:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual <b>10.0.101.254</b>.</li> <li>• Establezca la prioridad del grupo en <b>150</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 para disminuir en 60.</li> </ul> <p>Configure IPv4 HSRP grupo <b>124</b> para la VLAN 102:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual <b>10.0.102.254</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 para disminuir en 60.</li> </ul> <p>Configure IPv6 HSRP grupo <b>106</b> para la VLAN 100:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6 autoconfig</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 6 para disminuir en 60.</li> </ul> <p>Configure IPv6 HSRP grupo <b>116</b> para la VLAN 101:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6 autoconfig</b>.</li> <li>• Establezca la prioridad del grupo en <b>150</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 6 para disminuir en 60.</li> </ul> <p>Configure IPv6 HSRP grupo <b>126</b> para la VLAN 102:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6 autoconfig</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 6 para disminuir en 60.</li> </ul>

### Tarea 4.1

Se procede a configurar en D1 IP SLAs que prueben la accesibilidad de la interfaz R1 e0/1, se adjunta código:

#### Configuración D1

D1#configure terminal	entrada en configuración global
D1(config)#ip sla 4	configuración de SLA para ipv4
D1(config-ip-sla)# icmp-echo 10.0.10.1	ping a la ip del R1
D1(config-ip-sla-echo)# frequency 5	frecuencia del ping en segundos
D1(config-ip-sla-echo)# exit	salida de la configuración SLA
D1(config)#ip sla 6	configuración de SLA para ipv6
D1(config-ip-sla)# icmp-echo 2001:db8:100:1010:: 1	ping a la ip del R1
D1(config-ip-sla-echo)# frequency 5	frecuencia del ping en segundos
D1(config-ip-sla-echo)# exit	salida de la configuración SLA
D1(config)#ip sla schedule 4 life forever start-time now	programación SLA
D1(config)#ip sla schedule 6 life forever start-time now	programación SLA
D1(config)#track 4 ip sla 4	rastreo SLA
D1(config-track)# delay down 10 up 15	tiempo retraso del rastreo SLA
D1(config-track)# exit	salida configuración rastreo
D1(config)#track 6 ip sla 6	rastreo SLA
D1(config-track)# delay down 10 up 15	tiempo retraso del rastreo SLA
D1(config-track)# exit	salida configuración rastreo
D1(config)#end	sale al modo EXEC privilegiado
D1#copy running-config startup-config	salva la configuración

### Tarea 4.2

Se procede a configurar en D2 IP SLAs que prueben la accesibilidad de la interfaz R3 e0/1, se adjunta código:

#### Configuración D2

D2#configure terminal	entrada en configuración global
D2(config)#ip sla 4	configuración de SLA para ipv4
D2(config-ip-sla)# icmp-echo 10.0.11.1	ping a la ip del R1
D2(config-ip-sla-echo)# frequency 5	frecuencia del ping en segundos

D2(config-ip-sla-echo)# exit	salida de la configuración SLA
D2(config)#ip sla 6	configuración de SLA para ipv6
D2(config-ip-sla)# icmp-echo 2001:db8:100:1011:: 1	ping a la ip del R1
D2(config-ip-sla-echo)# frequency 5	frecuencia del ping en segundos
D2(config-ip-sla-echo)# exit	salida de la configuración SLA
D2(config)#ip sla schedule 4 life forever start-time now	programación SLA
D2(config)#ip sla schedule 6 life forever start-time now	programación SLA
D2(config)#track 4 ip sla 4	rastreo SLA
D2(config-track)# delay down 10 up 15	tiempo retraso del rastreo SLA
D2(config-track)# exit	salida configuración rastreo
D2(config)#track 6 ip sla 6	rastreo SLA
D2(config-track)# delay down 10 up 15	tiempo retraso del rastreo SLA
D2(config-track)# exit	salida configuración rastreo
D2(config)#end	sale al modo EXEC privilegiado
D2#copy running-config startup-config	salva la configuración

### Tarea 4.3

Se procede a configurar en D1 configure HSRPv2, se adjunta código:

#### Configuración D1

D1#configure terminal	entrada en configuración global
D1(config)#interface vlan 100	entrada en la interfaz vlan
D1(config-if)# standby version 2	versión del standby
D1(config-if)# standby 104 ip 10.0.100.254	configuración IP del standby
D1(config-if)# standby 104 priority 150	configuración de prioridad del standby
D1(config-if)# standby 104 preempt	configuración de preferencia del standby
D1(config-if)# standby 104 track 4 decrement 60	rastreo del objeto decremento 60
D1(config-if)# standby 106 ipv6 autoconfig	configuración del standby ipv6
D1(config-if)# standby 106 priority 150	configuración de prioridad del standby
D1(config-if)# standby 106 preempt	configuración de preferencia del standby
D1(config-if)# standby 106 track 6 decrement 60	rastreo del objeto decremento 60
D1(config-if)# exit	salida de la interfaz

D1(config)#interface vlan 101	entrada en la interfaz vlan
D1(config-if)# standby version 2	versión del standby
D1(config-if)# standby 114 ip 10.0.101.254	configuración IP del standby
D1(config-if)# standby 114 preempt	configuración de preferencia del standby
D1(config-if)# standby 114 track 4 decrement 60	rastreo del objeto decremento 60
D1(config-if)# standby 116 ipv6 autoconfig	configuración del standby ipv6
D1(config-if)# standby 116 preempt	configuración de preferencia del standby
D1(config-if)# standby 116 track 6 decrement 60	rastreo del objeto decremento 60
D1(config-if)# exit	salida de la interfaz
D1(config)#interface vlan 102	entrada en la interfaz vlan
D1(config-if)# standby version 2	versión del standby
D1(config-if)# standby 124 ip 10.0.102.254	configuración IP del standby
D1(config-if)# standby 124 priority 150	configuración de prioridad del standby
D1(config-if)# standby 124 preempt	configuración de preferencia del standby
D1(config-if)# standby 124 track 4 decrement 60	rastreo del objeto decremento 60
D1(config-if)# standby 126 ipv6 autoconfig	configuración del standby ipv6
D1(config-if)# standby 126 priority 150	configuración de prioridad del standby
D1(config-if)# standby 126 preempt	configuración de preferencia del standby
D1(config-if)# standby 126 track 6 decrement 60	rastreo del objeto decremento 60
D1(config-if)# exit	salida de la interfaz vlan
D1(config)#end	sale al modo EXEC privilegiado
D1#copy running-config startup-config	salva la configuración

## Configuración D2

D2#configure terminal	entrada en configuración global
D2(config)#interface vlan 100	entrada en la interfaz vlan
D2(config-if)# standby version 2	versión del standby
D2(config-if)# standby 104 ip 10.0.100.254	configuración IP del standby
D2(config-if)# standby 104 preempt	configuración de preferencia del standby
D2(config-if)# standby 104 track 4 decrement 60	rastreo del objeto decremento 60
D2(config-if)# standby 106 ipv6 autoconfig	configuración del standby ipv6



D2(config-if)# standby 106 preempt	configuración de preferencia del standby
D2(config-if)# standby 106 track 6 decrement 60	rastreo del objeto decremento 60
D2(config-if)# exit	salida de la interfaz
D2(config)#interface vlan 101	entrada en la interfaz vlan
D2(config-if)# standby version 2	versión del standby
D2(config-if)# standby 114 ip 10.0.101.254	configuración IP del standby
D2(config-if)# standby 114 priority 150	configuración de prioridad del standby
D2(config-if)# standby 114 preempt	configuración de preferencia del standby
D2(config-if)# standby 114 track 4 decrement 60	rastreo del objeto decremento 60
D2(config-if)# standby 116 ipv6 autoconfig	configuración del standby ipv6
D2(config-if)# standby 116 priority 150	configuración de prioridad del standby
D2(config-if)# standby 116 preempt	configuración de preferencia del standby
D2(config-if)# standby 116 track 6 decrement 60	rastreo del objeto decremento 60
D2(config-if)# exit	salida de la interfaz
D2(config)#interface vlan 102	entrada en la interfaz vlan
D2(config-if)# standby version 2	versión del standby
D2(config-if)# standby 124 ip 10.0.102.254	configuración IP del standby
D2(config-if)# standby 124 preempt	configuración de preferencia del standby
D2(config-if)# standby 124 track 4 decrement 60	rastreo del objeto decremento 60
D2(config-if)# standby 126 ipv6 autoconfig	configuración del standby ipv6
D2(config-if)# standby 126 preempt	configuración de preferencia del standby
D2(config-if)# standby 126 track 6 decrement 60	rastreo del objeto decremento 60
D2(config-if)# exit	salida de la interfaz vlan
D2(config)#end	sale al modo EXEC privilegiado
D2#copy running-config startup-config	salva la configuración

## Parte 5: Seguridad

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología.

Las tareas de configuración son las siguientes:

*Tabla 9: Tareas Parte 5*

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.	Contraseña: <b>cisco12345cisco</b>
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.	Detalles de la cuenta encriptada SCRYPT: <ul style="list-style-type: none"><li>• Nombre de usuario Local: <b>sadmin</b></li><li>• Nivel de privilegio <b>15</b></li><li>• Contraseña: <b>cisco12345cisco</b></li></ul>
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: <ul style="list-style-type: none"><li>• Dirección IP del servidor RADIUS es 10.0.100.6.</li><li>• Puertos UDP del servidor RADIUS son 1812 y 1813.</li><li>• Contraseña: <b>\$strongPass</b></li></ul>
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	Especificaciones de autenticación AAA: <ul style="list-style-type: none"><li>• Use la lista de métodos por defecto</li><li>• Valide contra el grupo de servidores RADIUS</li><li>• De lo contrario, utilice la base de datos local.</li></ul>
5.6	Verifique el servicio AAA en todos los dispositivos (except R2).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: <b>raduser</b> y la contraseña: <b>upass123</b> .

### **Tarea 5.1**

Se procede a configurar en todos los dispositivos, EXEC privilegiado usando el algoritmo de encriptación SCRYPT, con la contraseña **cisco12345cisco**, se adjunta código:

#### **Configuración R1**

```
R1#configure terminal
R1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
R1(config)# end
R1#copy running-config startup-config
```

#### **Configuración R2**

```
R2#configure terminal
R2(config)#enable algorithm-type SCRYPT secret cisco12345cisco
R2(config)# end
R2#copy running-config startup-config
```

#### **Configuración R3**

```
R3#configure terminal
R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco
R3(config)# end
R3#copy running-config startup-config
```

#### **Configuración D1**

```
D1#configure terminal
D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
D1(config)# end
D1#copy running-config startup-config
```

#### **Configuración D2**

```
D2#configure terminal
D2(config)#enable algorithm-type SCRYPT secret cisco12345cisco
D2(config)# end
```

D2#copy running-config startup-config

### **Configuración A1**

A1#configure terminal

A1(config)#enable algorithm-type SCRYPT secret cisco12345cisco

A1(config)# end

A1#copy running-config startup-config

### **Tarea 5.2**

Se procede a configurar en todos los dispositivos, un usuario local **sadmin** con privilegio **15** y contraseña **cisco12345cisco** y protéjalo usando el algoritmo de encriptación SCRYPT, se adjunta código:

### **Configuración R1**

R1#configure terminal

R1(config)#sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

R1(config)# end

R1#copy running-config startup-config

### **Configuración R2**

R2#configure terminal

R2(config)#sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

R2(config)# end

R2#copy running-config startup-config

### **Configuración R3**

R3#configure terminal

R3(config)#sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

R3(config)# end

R3#copy running-config startup-config

### **Configuración D1**

D1#configure terminal

```
D1(config)#sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
D1(config)# end
D1#copy running-config startup-config
```

### **Configuración D2**

```
D2#configure terminal
D2(config)#sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
D2(config)# end
D2#copy running-config startup-config
```

### **Configuración A1**

```
A1#configure terminal
A1(config)#sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
A1(config)# end
A1#copy running-config startup-config
```

### **Tarea 5.3**

Se procede a habilitar en todos los dispositivos (excepto R2) el AAA, se adjunta código:

### **Configuración R1**

```
R1#configure terminal
R1(config)#aaa new-model
R1(config)# end
R1#copy running-config startup-config
```

### **Configuración R3**

```
R3#configure terminal
R3(config)#aaa new-model
R3(config)# end
R3#copy running-config startup-config
```

### **Configuración D1**

```
D1#configure terminal
D1(config)#aaa new-model
D1(config)# end
D1#copy running-config startup-config
```

### **Configuración D2**

```
D2#configure terminal
D2(config)#aaa new-model
D2(config)# end
D2#copy running-config startup-config
```

### **Configuración A1**

```
A1#configure terminal
A1(config)#aaa new-model
A1(config)# end
A1#copy running-config startup-config
```

## **Tarea 5.4**

Se procede a configurar en todos los dispositivos (excepto R2) las especificaciones del servidor RADIUS, se adjunta código:

### **Configuración R1**

```
R1#configure terminal
R1(config)#radius server RADIUS
R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
R1(config-radius-server)# key $trongPass
R1(config-radius-server)# exit
R1(config)# end
R1#copy running-config startup-config
```

### **Configuración R3**

R1#configure terminal

R3(config)#radius server RADIUS

R3(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813

R3(config-radius-server)# key \$trongPass

R3(config-radius-server)# exit

R3(config)# end

R3#copy running-config startup-config

### **Configuración D1**

D1#configure terminal

D1(config)#radius server RADIUS

D1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813

D1(config-radius-server)# key \$trongPass

D1(config-radius-server)# exit

D1(config)# end

D1#copy running-config startup-config

### **Configuración D2**

D2#configure terminal

D2(config)#radius server RADIUS

D2(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813

D2(config-radius-server)# key \$trongPass

D2(config-radius-server)# exit

D2(config)# end

D2#copy running-config startup-config

### **Configuración D1**

A1#configure terminal

A1(config)#radius server RADIUS

A1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813

```
A1(config-radius-server)# key $strongPass
A1(config-radius-server)# exit
A1(config)# end
A1#copy running-config startup-config
```

## **Tarea 5.5**

Se procede a configurar en todos los dispositivos (excepto R2), la lista de métodos de autenticación AAA, se adjunta código:

### **Configuración R1**

```
R1#configure terminal
R1(config)#aaa authentication login default group radius local
R1(config)# end
R1#copy running-config startup-config
```

### **Configuración R3**

```
R3#configure terminal
R3(config)#aaa authentication login default group radius local
R3(config)# end
R3#copy running-config startup-config
```

### **Configuración D1**

```
D1#configure terminal
D1(config)#aaa authentication login default group radius local
D1(config)# end
D1#copy running-config startup-config
```

### **Configuración D2**

```
D2#configure terminal
D2(config)#aaa authentication login default group radius local
D2(config)# end
D2#copy running-config startup-config
```



### **Configuración A1**

A1#configure terminal

A1(config)#aaa authentication login default group radius local

A1(config)# end

A1#copy running-config startup-config

## Parte 6: Configure las funciones de Administración de Red

En esta parte, debe configurar varias funciones de administración de red.

Las tareas de configuración son las siguientes:

*Tabla 10: Tareas Parte 6*

Tarea#	Tarea	Especificación
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: <ul style="list-style-type: none"><li>• R1 debe sincronizar con R2.</li><li>• R3, D1 y A1 para sincronizar la hora con R1.</li><li>• D2 para sincronizar la hora con R3.</li></ul>
6.4	Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.
6.5	Configure SNMPv2c en todos los dispositivos excepto R2	Especificaciones de SNMPv2: <ul style="list-style-type: none"><li>• Únicamente se usará SNMP en modo lectura (Read-Only).</li><li>• Limite el acceso SNMP a la dirección IP de la PC1.</li><li>• Configure el valor de contacto SNMP con su nombre.</li><li>• Establezca el <i>community string</i> en <b>ENCORSA</b>.</li><li>• En R3, D1, y D2, habilite el envío de <i>traps config</i> y <i>ospf</i>.</li><li>• En R1, habilite el envío de <i>traps bgp</i>, <i>config</i>, y <i>ospf</i>.</li><li>• En A1, habilite el envío de <i>traps config</i>.</li></ul>

## **Tarea 6.1**

Se configura en todos los dispositivos, el reloj local a la hora UTC actual, se adjunta código.

### **Configuración R1**

```
R1#configure terminal
R1(config)#ntp server 2.2.2.2
R1#copy running-config startup-config
```

### **Configuración R3**

```
R3#configure terminal
R3(config)#ntp server 2.2.2.2
R3#copy running-config startup-config
```

### **Configuración D1**

```
D1#configure terminal
D1(config)#ntp server 2.2.2.2
D1#copy running-config startup-config
```

### **Configuración D2**

```
D2#configure terminal
D2(config)#ntp server 2.2.2.2
D2#copy running-config startup-config
```

### **Configuración A1**

```
A1#configure terminal
A1(config)#ntp server 2.2.2.2
A1#copy running-config startup-config
```

## **Tarea 6.2**

Se configura R2 como NTP maestro, se adjunta código.

### **Configuración R2**

```
R2#configure terminal
R2(config)#ntp master 3
R2(config)# end
R2#copy running-config startup-config
```

## **Tarea 6.3**

Se configura NTP en R1, R3, D1, D2, y A1, se adjunta código.

### **Configuración R1**

```
R1#configure terminal
R1(config)#ntp server 2.2.2.2
R1(config)# end
R1#copy running-config startup-config
```

### **Configuración R3**

```
R3#configure terminal
R3(config)#ntp server 2.2.2.2
R3(config)# end
R3#copy running-config startup-config
```

### **Configuración D1**

```
D1#configure terminal
D1(config)#ntp server 2.2.2.2
D1(config)# end
D1#copy running-config startup-config
```

### **Configuración D2**

```
D2#configure terminal
D2(config)#ntp server 2.2.2.2
```

```
D2(config)# end
D2#copy running-config startup-config
```

### **Configuración A1**

```
A1#configure terminal
A1(config)#ntp server 2.2.2.2
A1(config)# end
A1#copy running-config startup-config
```

### **Tarea 6.4**

Se configura Syslog en todos los dispositivos excepto R2, se adjunta código.

### **Configuración R1**

```
R1#configure terminal
R1(config)# logging trap warning
R1(config)# logging host 10.0.100.5
R1(config)# logging on
R1(config)# end
R1#copy running-config startup-config
```

### **Configuración R3**

```
R3#configure terminal
R3(config)# logging trap warning
R3(config)# logging host 10.0.100.5
R3(config)# logging on
R3(config)# end
R3#copy running-config startup-config
```

### **Configuración D1**

```
D1#configure terminal
D1(config)# logging trap warning
D1(config)# logging host 10.0.100.5
```

```
D1(config)# logging on
D1(config)# end
D1#copy running-config startup-config
```

### **Configuración D2**

```
D2#configure terminal
D2(config)# logging trap warning
D2(config)# logging host 10.0.100.5
D2(config)# logging on
D2(config)# end
D2#copy running-config startup-config
```

### **Configuración A1**

```
A1#configure terminal
A1(config)# logging trap warning
A1(config)# logging host 10.0.100.5
A1(config)# logging on
A1(config)# end
A1#copy running-config startup-config
```

### **Tarea 6.5**

Se configura SNMPv2c en todos los dispositivos excepto R2, se adjunta código.

### **Configuración R1**

```
R1#configure terminal
R1(config)#ip access-list standard SNMP-NMS
R1(config-std-nacl)# permit host 10.0.100.5
R1(config-std-nacl)# exit
R1(config)# snmp-server contact Cisco Student
R1(config)# snmp-server community ENCORSA ro SNMP-NMS
R1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
R1(config)# snmp-server ifindex persist
```

```
R1(config)# snmp-server enable traps bgp
R1(config)# snmp-server enable traps config
R1(config)# snmp-server enable traps ospf
R1(config)# end
R1#copy running-config startup-config
```

### **Configuración R3**

```
R3#configure terminal
R3(config)#ip access-list standard SNMP-NMS
R3(config-std-nacl)# permit host 10.0.100.5
R3(config-std-nacl)# exit
R3(config)# snmp-server contact Cisco Student
R3(config)# snmp-server community ENCORSA ro SNMP-NMS
R3(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)# snmp-server ifindex persist
R3(config)# snmp-server enable traps bgp
R3(config)# snmp-server enable traps config
R3(config)# snmp-server enable traps ospf
R3(config)# end
R3#copy running-config startup-config
```

### **Configuración D1**

```
D1#configure terminal
D1(config)#ip access-list standard SNMP-NMS
D1(config-std-nacl)# permit host 10.0.100.5
D1(config-std-nacl)# exit
D1(config)# snmp-server contact Cisco Student
D1(config)# snmp-server community ENCORSA ro SNMP-NMS
D1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)# snmp-server ifindex persist
D1(config)# snmp-server enable traps bgp
```

```
D1(config)# snmp-server enable traps config
D1(config)# snmp-server enable traps ospf
D1(config)# end
D1#copy running-config startup-config
```

## **Configuración D2**

```
D2#configure terminal
D2(config)#ip access-list standard SNMP-NMS
D2(config-std-nacl)# permit host 10.0.100.5
D2(config-std-nacl)# exit
D2(config)# snmp-server contact Cisco Student
D2(config)# snmp-server community ENCORSA ro SNMP-NMS
D2(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)# snmp-server ifindex persist
D2(config)# snmp-server enable traps bgp
D2(config)# snmp-server enable traps config
D2(config)# snmp-server enable traps ospf
D2(config)# end
D2#copy running-config startup-config
```

## **Configuración A1**

```
A1#configure terminal
A1(config)#ip access-list standard SNMP-NMS
A1(config-std-nacl)# permit host 10.0.100.5
A1(config-std-nacl)# exit
A1(config)# snmp-server contact Cisco Student
A1(config)# snmp-server community ENCORSA ro SNMP-NMS
A1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
A1(config)# snmp-server ifindex persist
A1(config)# snmp-server enable traps bgp
A1(config)# snmp-server enable traps config
```



```
A1(config)# snmp-server enable traps ospf
```

```
A1(config)# end
```

```
A1#copy running-config startup-config
```

## **CONCLUSIONES**

El empleo de RADIUS nos permite lograr una autenticación que no se aloje directamente en el dispositivo consultado, y se realice dicho proceso con un equipo remoto en el cual se encuentren los datos del usuario, nombre, contraseña, nivel de uso, entre otros.

HSRP debe ser utilizado siempre a nivel corporativo, ya que evita que perdamos salida de la red en la que se encuentre el host a otras redes, ya que esto fortalece el soporte a fallos si algún dispositivo que funciones de puerta de enlace falla.

El empleo del protocolo LACP, garantiza una conexión redundante y confiable, ya que suma las velocidades de los enlaces que participen, es fundamental en la implementación de una topología de core.

Gracias al uso de protocolos de enrutamiento dinámico nos permite el aprendizaje rápido de la topología de red por la cual estemos pasando y la cantidad de saltos posibles para alcanzar un destino.

## BIBLIOGRAFIA

Configuración DHCP en Router (s.f), 27 de mayo de 2018, recuperado de <https://apuntesdecisco.blogspot.com/2008/07/configuracin-de-dhcp-en-lrouter.html>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115.

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115.

Gerometta Oscar, (2015), 28 de junio, Que es una SVI, recuperado de <http://librosnetworking.blogspot.com/2015/06/que-es-una-svi.html>

HSRP Versión 2 (s.f), 27 mayo de 2018, recuperado de [https://www.cisco.com/c/en/us/td/docs/ios-ml/ios/ipapp\\_fhrp/configuration/xs3s/fhp-xe-3s-book/fhp-hsrp-v2.html](https://www.cisco.com/c/en/us/td/docs/ios-ml/ios/ipapp_fhrp/configuration/xs3s/fhp-xe-3s-book/fhp-hsrp-v2.html)

Morales, J. M. Introduccción al CLI en routers y switches cisco. Recuperado de: <https://pics.unlugarenelmundo.es/hechoencasa/CLI%20en%20Routers%20y%20Switches%20Cisco.pdf>